Ania
Associazione Nazionale
fra le Imprese Assicuratrici

Queen Mary
University of London

BTG LEGAL
Batini Traverso Grasso & Associati

CMI AND MARINE CYBERSECURITY:

WHERE ARE WE ?

ALBERTO BATINI

BTG LEGAL

GLOBAL INSURANCE LAW CONNECT

ANIA MILAN 5th JUNE 2024

BTG LEGAL
Batini Traverso Grasso & Associati

AGENDA

INTRODUCTION

THE SOLAS CONVENTION

THE QUESTIONNAIRE

WHAT'S NEXT

INTRODUCTION

HOW DID WE GET HERE

The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

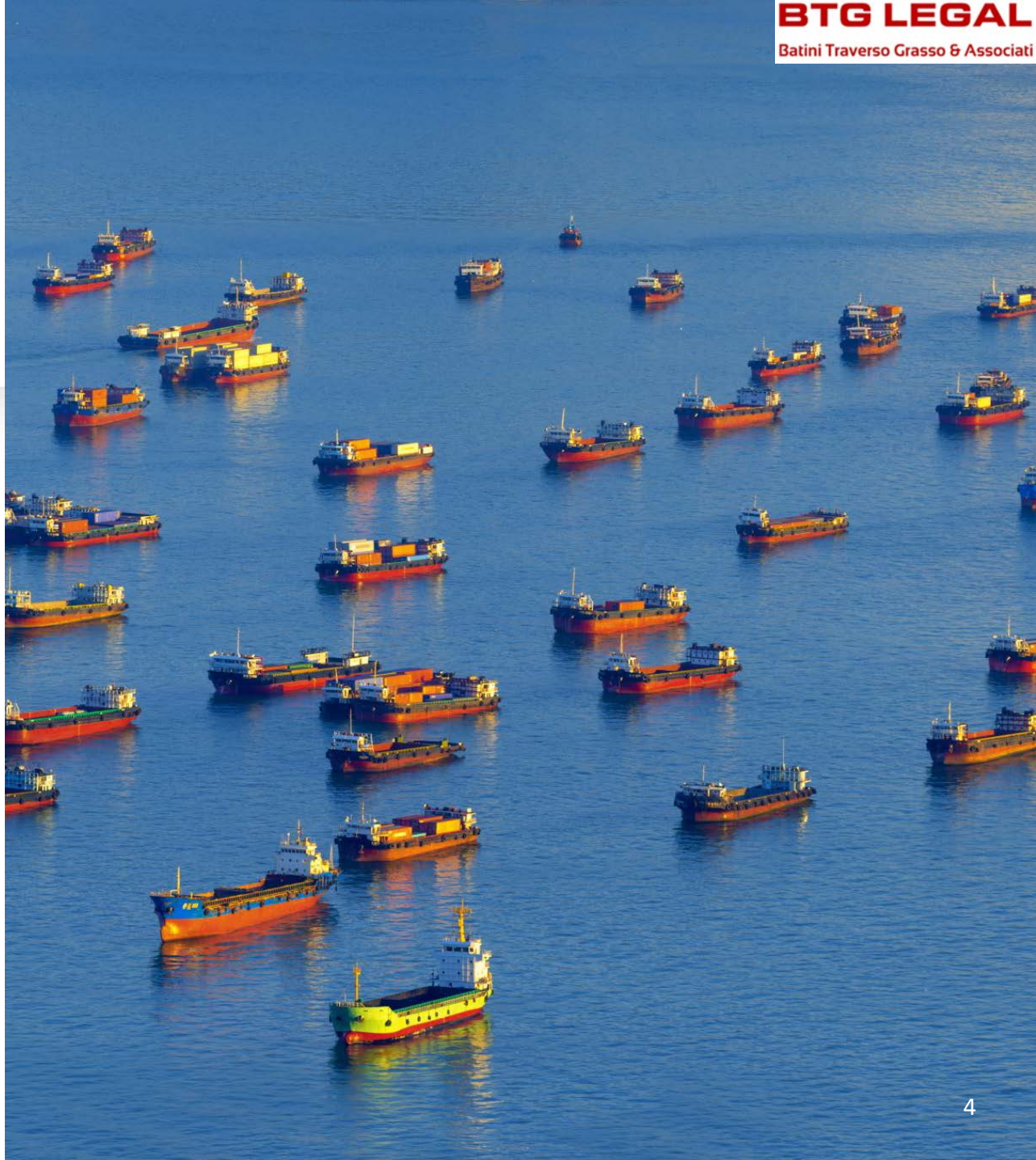
The CMI's Cybercrime in Shipping IWG was formed after the New York Conference in 2016 during which an informative session was held on the topic. The original purpose of the Group was to monitor and research this crucial area of shipping and its effect on legalities. At the Montreal Colloquium in 2023, the IWG decided to proceed with the drafting of a questionnaire to be submitted to the national associations of maritime law. The speech will synthetically update on the progress of the work of the IWG in this respect and on the intentions to coordinate the works of the IWG on the autonomous vessels, which presents several similarities of discipline.

THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA (SOLAS)

- The International Convention for the Safety of Life at Sea (SOLAS) is an international maritime treaty which sets out minimum safety standards in the construction, equipment and operation of merchant ships. The International Maritime Organization convention requires signatory flag states to ensure that ships flagged by them comply with at least these standards.

- Initially prompted by the sinking of the Titanic, the current version of SOLAS is the 1974 version, known as SOLAS 1974, which came into force on 25 May 1980,[1] and has been amended several times. As of April 2022, SOLAS 1974 has **167 contracting states**, which flag about **99% of merchant ships** around the world in terms of gross tonnage.

- SOLAS in its successive forms is generally regarded as the most important of all international treaties concerning the safety of merchant ships.



THE IWG QUESTIONNAIRE

LET'S DIVE IN

GENERAL ISSUES

General

1. To what extent do you agree with the following statement: “existing international convention adequately meets cyber risk ?”

   1 = strongly disagree; 2 = disagree; 3 = neutral; 4 = agree; 5 = strongly agree

2. To what extent do you agree with the following statement: “either a new standalone cyber convention or amendment to existing conventions is required to address cyber risk ?”

   1 = strongly disagree; 2 = disagree; 3 = neutral; 4 = agree; 5 = strongly agree

3. To the extent you believe that existing international conventions do not adequately cover cyber risk, do you believe this would best be rectified by:
   a. A new bespoke cyber risk convention.
   b. Amendment to various existing international conventions.
   c. An addition to SOLAS covering cyber risk.

INSURANCE RELATED ISSUES

1. How is cyber risk perceived in your country by the maritime industry? Is it a kind of risk that shipping business feels the need to transfer to the insurance market?

2. Did Members and Affiliates in your organization experience cyber disputes with third parties or their insurers? Are they experiencing any such dispute at present?

3. Would the maritime industry in your country welcome a standalone marine insurance product covering cyber risks of shipowners, charterers or maritime industry operators (such as terminal operators), also in the light of the need to comply with IMO's 2021 cyber requirements, and to protect themselves against claims under BIMCO's Cyber Security Clause 2019?

4. Are there already in your country standalone marine cyber insurance products (standalone cyber risk policies covering both first- and third-party costs) associated with incidents ranging from online extortion and data breaches to network outages and social engineering, being sold on the market or are you aware of any such products?

5. Do you think that the extent of marine cyber insurance cover provided in the products available on the market is substantially uniform and homogenous in terms of risks covered, limits and sub-limits of cover, exclusions, and warranties? In the negative, do you think that the differences and inhomogeneity of scope of cover in this type of product is such to generate future coverage litigation?

INSURANCE RELATED ISSUES

- 6) In your opinion is there a marine industry demand for coverage of those risks presently carved out from H&M and Cargo Insurance Policies, by way of either the Clause 380 - Institute Cyber Attack Exclusion Clause [10/11/2003] or LMA5403 - Marine Cyber Endorsement [11/11/19] ?
- 7) Do you think that all or some of the following should deserve an internationally uniform definition, in general or within the context of the maritime industry, to reduce uncertainties and litigation:
- (i) Nature, scope, and extent of a cyber risk;
- (ii) Definition of “Cyber”
- (iii) Definition of “Cyber-Attack”;
- (iv) Addressing the growing gap between the coverage offered by stand-alone named peril cyber policies and the broad cyber exclusions being built into other lines of coverage;
  - Extent of Insured’s obligation to prevent a cyber-attack and enforce and maintain an adequate cyber prevention program for their ships, cargo carrying equipment, terminal operations or the like, in other words a cyber-hygiene attitude. In particular, whether abidance by the Insured to IMO MSC-FAL.1-Circ.3-Rev.2 Guidelines on maritime cyber risk management, to Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems and to ISO 27000 standards, should be construed as policy warranties.
  - Limitation of liability of shipowners and ship operators for damages against third parties arising out of cyber-attacks or cyber related incidents;
  - Extent of liability of Insurers on silent cyber claims, meaning those that arose from non-affirmative risks, that is, risks that were neither explicitly included in nor explicitly excluded from an insurance policy. Addressing these silent risks would provide both carriers and their customers with greater clarity but it would also significantly shrink the potential coverage for cyber risks tied to other lines of coverage, such as property, or crime.
  - Relation between cyber insurance and war and terrorism related risks and insurance;
  - Relation between cyber insurance and other classes of insurance or policies;
  - Role of Government in managing cyber risks, since the scope of the cyber exposures is too broad to be solved by the private sector alone.

INSURANCE RELATED ISSUES

8) Do you think that there is a demand from the maritime industry in your jurisdiction for a direct action against Insurers in marine cyber disputes or, at least, in some cases of marine cyber disputes?

9) In your judgement and after having shared the opinions of your associates and affiliates, does your organization think that a lack of historical data, a lack of ability to predict the future of cyber risk, the possibility of large cascading loss events, and uncertainties among market participants about what is specifically covered under such policies all suggest that the matter should be regulated by a uniform piece of legislation? In the affirmative, which instrument would you think would be more efficient in regulating the matter? A soft law instrument (such as a Model Law), an Annex to SOLAS or an International Convention?

10) With the above in mind do you think that CMI should also apply to join the Joint Industry Working Group (JIWG) on Cyber Security spearheaded by BIMCO to merge forces on this issue?

11) Do you think that cyber safety and autonomous shipping are sufficiently related, not only in relation to insurance issues, to deserve a joint CMI working effort to achieve a more comprehensive target on the subject matter?

PORTS

1. How many known cyber-attacks have occurred in the maritime sector in your country in the last five years? Include attacks on vessels, port facilities or organisations in the logistics supply chain.

2. Are any M.A.S.S. vessels registered in your national ship registry?

3. To what extent has automation and digital technology been implemented in the training of seafarers in your country?

4. To what extent do you agree with the following statements about levels of automation and digital transformation in the maritime sector in your country?

1 = strongly disagree; 2 = disagree; 3 = neutral; 4 = agree; 5 = strongly agree

(a) There is an increasing integration and convergence between Information Technology ('IT') and Operational Technology ('OT') systems and assets;

(b) All maritime organisations are connected to the internet;

(c) Paper processes have been replaced by digitalisation;

(d) Automation has replaced previously manual cargo handling operations;

(e) EDI platforms are in widespread use;

(f) A maritime single window has been set up/will be in operation by the time resolution FAL.14(46) enters into force on 1/1/2024.

(g) EDI/MSW system architecture is adequately secured against cyber risk;

(h) Big data analytics are widely used to monitor and evaluate safety, security, energy efficiency and to optimize commodity flows;

(i) Cloud computing solutions are widely used;

(j) Cloud computing solutions offer secure, local data storage;

(k) The Internet of Things has been fully embraced by the maritime sector;

PORTS

5. How would you describe the extent of sector awareness of cyber-risks amongst maritime sector stakeholders in your country?
6. What measures are being taken in your country to raise awareness? Please indicate if these measures are being taken by government or by private organisations or both.
7. Which government department is responsible for the implementation of the SOLAS in your country?
8. Has this government department issued any regulation/communique on the implementation of legal requirements in your country under MSC Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems?
   If so, is there a mandatory requirement in force for implementation of Res. 428(98) in safety management systems (SMS) [*no later than the first annual verification of the company's Document of Compliance after 1 January 2021*] for:
   (a) vessels flying your country's national flag (yes/no)
   (b) foreign flagged vessels calling on a port in your country? (yes/no)
9. Has this government department issued any communique on sector guidelines/best practice in relation to cyber risk management, including:
   (a) IMO MSC-FAL.1-Circ.3-Rev.2 Guidelines on maritime cyber risk management;
   (b) Guidelines on Cyber Security on board Ships issued by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss;
   (c) Consolidated IACS Recommendation on cyber resilience (Rec. 166);
   (d) IAPH cybersecurity guidelines for ports & port facilities & IAPH Port Community Cyber Security Report;
   (e) Other (please specify).

PORTS

10. Are any of the following standards in widespread use in the maritime sector in your country?
    (a) ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. (ISO/IEC)
    (b) Network and Information Systems Regulations (2018) and NIS Directive (EU & UK);
    (c) United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).
    (d) Other? (please specify)

11. Is the port authority/any other port organisation in your country a member of IAPH?
    (a) Yes, regular member. (Please specify name of authority/organisation)
    (b) Yes, associate member. (Please specify name of authority/organisation)
    (c) No

12. What government department(s) are responsible for the prevention, detection, investigation or prosecution of cyber-attacks in your country?

13. If multiple government departments have roles and responsibilities in this area, is there any department/organisation that co-ordinates the work being done by these various entities?

14. Has government published a port sector cyber-security plan/policy/code of practice for your country?
    If yes, please specify & provide URL link to instrument/PDF copy

15. Has the port authority in your country published a port facility security plan as required under the ISPS Code (or its national equivalent regulation)?

PORTS

16. To what extent does the PFSP set out cyber risk management procedures?
    (a) Not mentioned
    (b) Not adequately addressed
    (c) Adequately addressed
    (d) Comprehensively addressed
    (e) Very comprehensively addressed
    (f) N/a - no PFSP
    (g) Unknown if there is a PFSP

17. Does the PFSP impose requirements to report & respond to cyber security threats, incidents & breaches?
    (a) Not mentioned
    (b) Not adequately addressed
    (c) Adequately addressed
    (d) Comprehensively addressed
    (e) Very comprehensively addressed
    (f) N/a - no PFSP
    (g) Unknown if there is a PFSP

18. Do Port Facility Security Officers include cyber risk prevention and response in the training, drills or exercises conducted on port facility security?
    (a) Not included
    (b) Not adequately addressed
    (c) Adequately addressed
    (d) Comprehensively addressed
    (e) Very comprehensively addressed
    (f) N/a - no training conducted.
    (g) Unknown if there is port facility security training conducted

PORTS

19 In your judgement and after having shared the opinions of your associates and affiliates, does your organization think that port facility cyber security is an issue that:

(a) is adequately regulated under the current framework of the ISPS, national law and /or sector standards; or
(b) should be regulated by a uniform international instrument
If in the affirmative, which instrument would you think would be more efficient in regulating the matter?
(i) A soft law instrument (such as a Model Law),
(ii) an Annex to the SOLAS, or other International Convention (please specify).

20 In your judgement and after having shared the opinions of your associates and affiliates, does your organization think that port facility cyber security is an issue that:

(a) is adequately regulated under the current framework of the ISPS, national law and /or sector guidelines; or
(b) should be regulated by a uniform international instrument
If in the affirmative, which instrument would you think would be more efficient in regulating the matter?
(i) A soft law instrument (such as a Model Law),
(ii) an Annex to the SOLAS, or other International Convention (please specify).

PORTS

21. In your judgement and after having shared the opinions of your associates and affiliates, does your organization think that cyber security on board ships is an issue that:

(a) is adequately regulated under the current framework of IMO regulations, national law and /or sector guidelines; or
(b) should be regulated by a uniform international instrument

If in the affirmative, which instrument would you think would be more efficient in regulating the matter?

(i) A soft law instrument (such as a Model Law),
(ii) an Annex to the SOLAS, or other International Convention (please specify).
(iii) Update of IMO Guidelines on Maritime Cyber Risk Management;

BTG LEGAL
Batini Traverso Grasso & Associati

WHAT'S NEXT

LOOKING AHEAD

BTG LEGAL
Batini Traverso Grasso & Associati

THE NATIONAL MARITIME LAW ASSOCIATIONS RESPONSES AND FURTHER ACTIONS FROM THE IWG

BTG LEGAL

Batini Traverso Grasso & Associati

THANK YOU

ALBERTO BATINI

+39 348 7902191

a.batini@btglegal.it

WWW.BTGLEGAL.IT